

Dec 02, 2020

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)CyberTip Report 74930637 currently in the custody of the
Federal Bureau of Investigations (FBI), Milwaukee Office,
and more fully described in Attachment A, attached hereto.

Case No. 20-M-456 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the
person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|-----------------------------------|--|
| 18 U.S.C. Sections 2252 and 2252A | Possessing and distribution of child pornography |

The application is based on these facts:
See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TFO [Signature]

Applicant's signature

FBI Task Force Officer Daniel Chmielewski

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 12-2-20

City and state: Milwaukee, WI

[Signature]

Judge's signature

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Task Force Officer Daniel Chmielewski, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer (TFO) with the United States Department of Justice, Federal Bureau of Investigation (FBI), for the Child Exploitation and Human Trafficking Task Force. I have been employed as a law enforcement officer since 2013 and have been assigned as a TFO since March 2020. As such, I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, § 2510 (7). That is, I am an officer of the United States, who is empowered by law to conduct investigations regarding violations of United States law, to execute warrants issued under the authority of the United States, and to make arrests of the offenses enumerated in Title 18, United States Code, § 2251, *et. seq.* In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and child pornography. I have previously been involved in criminal investigations concerning violations of federal and state laws.

2. Since joining law enforcement, your affiant has received specialized training in child pornography investigations, identifying and seizing electronic evidence, computer forensics, recovery, and social media investigations. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

3. This affidavit is submitted in support of an application for a search warrant for the files submitted in connection with a cybertip (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in

Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5).

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A are located in the place described in Attachment A.

5. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

6. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

7. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B to this Affidavit.

9. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a

minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

10. “Visual depictions” includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image *See* 18 U.S.C. § 2256(5).

CYBERTIP

11. The National Center for Missing and Exploited Children (“NCMEC”) is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a company providing services on the internet (“ISP”) can go to an online portal that NCMEC has set up for the submission of these tips. The ISP then can provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ISP provides is voluntary and undertaken at the initiative of the reporting ISP. The ISP may also upload to NCMEC any files it collected in connection with the activity. The ISP may or may not independently view the content of the files it uploads. NCMEC does not review the content of these uploaded files. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP provides

such as IP addresses. NCMEC then packages the information from the ISP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

12. On July 20, 2020, Microsoft completed a Cybertip to NCMEC. The Cybertip number was **74930637**. Microsoft reported that a OneDrive account with an electronic service provider user ID number of, “30000301e2889,” uploaded 25 files, which Microsoft classified as apparent child pornography on July 19, 2020, at 22:40 hours (UTC). The files were not reviewed by NCMEC or Microsoft but were classified based on hash value.

13. I know from my training and experience that the ISP flags and reports images or files that have the same “hash values” as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is similar to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

14. Here, I know from my training and experience that the ISP compares the hash values of files that its customers transmit on its systems against the list of hash values that NCMEC has. If the ISP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ISP’s systems.

15. I also know that the ISP uses PhotoDNA. PhotoDNA is a software technology developed by Microsoft that computes hash values of images, video and audio files to identify alike images.

PhotoDNA is primarily used in the prevention of child pornography proliferation. Here, that technology was used to determine that a user of its services posted or transmitted a file with the same hash value as an image that has previously identified as containing child pornography.

16. The IP address associated with the OneDrive uploads was 184.58.138.130. Based on the geo-location of the IP address, NCMEC forwarded the tip to the Wisconsin Department of Justice Department of Criminal Investigations (DCI). DCI conducted an administrative subpoena to Charter Communications and located a subscriber name of Larry Theurich, with an address of, W303 S2789 Bethesda Circle in the Town of Genesee, Waukesha County, Wisconsin. Based on the address, DCI forwarded the information to the Waukesha County Sheriff's Department (WKSO), which is an internet crimes against children affiliate agency.

17. On September 9, 2020, WKSO Detective Mark Conrad received and reviewed **CyberTip 74930637**. Detective Conrad reviewed the uploaded photograph files in question and provided the following details:

18. "... I also reviewed the images attached to the tip. I noted that all 25 appear to show apparent child pornography. Two images of note are described as an infant female being sexually assaulted with a screwdriver and a ballpoint pen or marker. Another image depicts an adult male sexually assaulting an infant female. The other images contained within the tip depicts similar images of both male and female children being sexually assault and/or exposing their genital areas."

19. During the course of the investigation, Detective Conrad found that Larry has a brother named, Eric P. Theurich, and that Eric had registered a vehicle at the above address. Detective Conrad further found out that Eric is a convicted sex offender, had recently served time in prison for possession of child pornography, and was on parole.

20. Detective Conrad made contact with Eric's parole agent, Jennifer Uppena, who stated that Eric is on active GPS monitoring and that he resides at a location called, "Cesar's Inn," located at 5527 W. National Ave. in West Milwaukee, Milwaukee County, Wisconsin. Jennifer stated that Eric stays every 7 to 10 days at Larry's residence in the Town of Genesee. Jennifer checked the GPS records for Eric and found that on the day of the illegal uploads, July 19, 2020, Eric was at Larry's residence in the Town of Genesee, Waukesha County, Wisconsin.

CONCLUSION

21. Based on the facts set forth above, your affiant believes probable cause exists that located within the referenced **CyberTip 74930637**, stored on a computer at the Federal Bureau of Investigation, Milwaukee, located at 3600 S. Lake Dr., St. Francis, Wisconsin, 53235, there are violations of Title 18, United States Code, §2252A(a)(2) and §2252A(a)(5)(B), which prohibits the knowing receipt or distribution of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) in interstate or foreign commerce, and the knowing possession of an image of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) that have traveled in interstate or foreign commerce or were produced using material so transported or shipped.

22. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of such violations will be found in the **CyberTip 74930637**, stored at the premises of Federal Bureau of Investigation, Milwaukee, located at 3600 S. Lake Dr., St. Francis, Wisconsin, 53235 (more precisely described in Attachment A.)

23. Accordingly, your affiant requests that a search warrant be issued authorizing FBI agents, representatives of the FBI, with assistance from representatives of other law enforcement agencies as required, to search items contained at the Federal Bureau of Investigation, Milwaukee, located at 3600 S. Lake Dr., St. Francis, Wisconsin, 53235 (more precisely described in Attachment A), for evidence, fruits, and instrumentalities (more precisely described in Attachment B) of the offenses described in paragraphs 6 and 7 of this affidavit.

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

Content of files uploaded in connection with Cybertip Report #74930637 (hereinafter and in Attachment B the “File(s)”), currently held by the FBI Milwaukee Office located at 3600 S. Lake Dr., St. Francis, Wisconsin, 53235.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

For the File(s) listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5):

1. Images or visual depictions of child pornography.
2. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors.
3. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the File(s), or that aid in the identification of persons involved in violations of 18 U.S.C. §§ 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5).

DEFINITIONS

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer data or electronic storage; any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as digital image files; microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. “Child Pornography” is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

6. “Visual depiction” includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).